

CLAIMS

1. A data communication apparatus having a memory space, the data communication apparatus managing the memory space by separating the memory space into one or more file systems, the apparatus comprising:

    authenticating means for requesting performance of one of a mutual authentication and a verification for a security code for each file system to be accessed from an external apparatus or a program;

    authentication information managing means for managing, for each file system, whether the file system is in an authentication-required state in which performance of one of the mutual authentication and the verification for the security code is requested or in a release state in which the access is permitted after the one of the mutual authentication and the verification for the security code is completed; and

    state managing means for returning the file system from the release state to the authentication-required state in response to an occurrence of a predetermined event.

2. The data communication apparatus according to Claim 1, wherein, when one of the external apparatus and the program changes the accessing file system to another file system, the state managing means resets the release state of the

original accessing file system to the authentication-required state.

3. The data communication apparatus according to Claim 1, wherein the state managing means resets the release state of the original accessing file system to the authentication-required state after a predetermined period of time has elapsed since the file system was changed to the release state or after a predetermined period of time has elapsed since the data communication apparatus was powered on.

4. A method for managing a memory of a data communication apparatus, the data communication apparatus having a memory space and managing the memory space by separating the memory space into one or more file systems, the method comprising the steps of:

(a) requesting performance of one of a mutual authentication and a verification for a security code for each file system to be accessed from an external apparatus or a program;

(b) managing, for each file system, whether the file system is in an authentication-required state in which performance of one of the mutual authentication and the verification for the security code is requested or in a release state in which the access is permitted after one of

the mutual authentication and the verification for the security code is completed; and

(c) returning the file system from the release state to the authentication-required state in response to an occurrence of a predetermined event.

5. The method for managing a memory of a data communication apparatus according to Claim 4, wherein, when one of the external apparatus and the program changes the accessing file system to another file system, step (c) resets the release state of the original accessing file system to the authentication-required state.

6. The method for managing a memory of a data communication apparatus according to Claim 4, wherein step (c) resets the release state of the original accessing file system to the authentication-required state after a predetermined period of time has elapsed since the file system was changed to the release state or after a predetermined period of time has elapsed since the data communication apparatus was powered on.